10.0 Safety Culture in the Nuclear Power Industry

Mr. Edward R. Frederick, Corrective Action Process Supervisor,
Three Mile Island Nuclear Generating Station,
Middleton, Pennsylvania, USA

The Way We Were

- Protect against the big problem, and that should cover the small problems that may arise
- Provide detailed procedures for each anticipated problem
- Train the operators about the theory underlying the systems and the details of system design and construction

Protect against the Big Problem

- Our anticipated big problem was a large leak in the Reactor Coolant System
- The protection for this consists of several independent methods of injecting water into the system to replace that which leaks out
- As long as these systems functioned on demand, the reactor would be protected from damage

Detailed Procedures

- The procedures were written such that if an operator could identify the failure; the appropriate recovery steps would be provided in the procedure
- All of the training, memorizing and simulating was aimed at identification of the failure and initiation of the appropriate recovery procedure

Operator Training

- The operator's training was heavily loaded with system design and interaction information
- The belief was that if something unexpected occurred, the operators would be able to improvise a solution

Arrogance in Design

It's not going to happen

Inability to observe fundamental parameter

- The fundamental safety rule is to keep the core cool
- There were no temperature indicators in the core
- Core temperature was inferred from water temperature at the exit of the reactor vessel - it assumes forced flow through the core

Inability to see the problem

- Core damage would be indicated by temperatures above the boiling point for the given pressure
- No instrumentation for boiling conditions
- No temperature instruments ranged above normal operating range (700F)

Ambiguity in displays

- The back-up cooling system was intended to provide cool water flow to the boilers to remove heat from the core
- There were no flow indicators for that system - flow was inferred from having the pumps turned on and the valves open

Flaws in controls & displays

- A relief valve was installed to reduce the upward pressure excursion anticipated on a loss of heat sink. It was expected that the valve would open briefly
- No direct position indication was provided for the relief valve even though it was known to fail frequently - valve position was inferred from the "demand" signal

Mistakes in Design

Failure to test the design assumptions in the real world

The alarm system

- Over 1300 alarm indicators were available in the control room on overhead panels.
- The alarms were not prioritized, color coded nor logically grouped
- Each alarm was labeled with a phrase describing a failure or unwanted condition
- The alarms were linked to a klaxon horn which sounded each time a new alarm was activated

The "computer"

- A "computer" was available to list the alarms as they actuated
- The output of the computer was an IBM Selectric Typewriter with tractor feed paper
- The typer often jammed
- It was unable to type more than about 6 lines of text per minute

Opacity

- no visual feedback
- no audio feedback
- no feel for the machine

Operation by exception

- the operator's mental model of the plant is modified by exception to normal system operation
- The assumption in the model is that the component and system are functioning normally unless the instruments or alarms provide an exception.

All of this and more

- Industry's safety assumption
- Flawed procedures
- Subjective training goals
- Instrumentation flaws and omissions

- . . . And the human element

Dr. Reason's Irony

- **". . . it is an irony of automation that we drill operators to follow written instructions and then put them in a system for the sole purpose of providing knowledge-based intelligence and IMPROVISATION."**

A new approach

AA Safety Culture grows slowly

Improved Instrumentation

- Wide range temperature indication installed in the reactor core
- Real-time boiling point information displayed and minimum margin established
- Secondary instrumentation added to the relief valve to indicate position

Improved instrumentation

- Enhanced meter face designs & digital
- key parameter cluster graph displays
- improved flow mimicking on panels
- control room & plant re-labeled
- prioritization of alarm system
- three new computers with multiple display
- increased staffing

New ideas

- Several systems upgraded to "safety grade" - better instrumentation and design
- audio and visual instrumentation added to the control room

Improved Procedures

- Symptom-based procedures introduced

A new Safety Culture

- Self reporting of problems
- application of resources to solve problems
- development of a learning organization

New tools

- On-site replica simulators mandatory
- Industry communication tools developed
- Accredited training centers established

Corrective Action Process

- INPO learned it from the airline industry in 1984
- Began development at TMI in 1988
- Infant system in 1992
- Effective system in place in 1996
- Continue to refine and improve